REMARKS

The Final Office Action of October 17, 2008 has been received and carefully reviewed. It is submitted that all bases of rejection are traversed and overcome. Claims 1-25 remain in the application. Claims 18-25 are allowed. Reconsideration of claims 1-17 is respectfully requested.

Claim 17 was identified as "currently amended" in Applicant's amendment filed December 21, 2007, and the word "and" was therein added after the penultimate paragraph. Claim 17 was identified as "previously presented" in the amendment filed June 18, 2008, however, the word "and" was inadvertently omitted from claim 17 in that listing of claims. The word "and" has been correctly added back into claim 17 in the listing of claims herein.

Claims 1-17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Droms et al. (U.S. Patent No. 7,143,435) in view of Donaldson (U.S. Patent No. 7,249,175). The Examiner considered Applicant's arguments and provided a response. Applicant respectfully submits that the Examiner's response reveals a misunderstanding of Applicant's arguments and claims. Applicant is providing the following to assist the Examiner in understanding why his invention as claimed is patentably distinguished over the cited art.

The Examiner states that Droms "...further disclosed a method for checking the message for user names (user identification) and URL (domain names) by the DNS to process the request from host (col 12, lines 50-67, col 13, lines 1-24, Figs 1-2)." Applicant acknowledges that Droms uses a DNS to check a requested URL (including a domain name) and "finds an IP address that is associated with the name, if any." (Col. 12, lines 53 – 59.) Droms provides an illustration which restricts access to the outside internet by using DHCP to configure certain hosts to use a DNS that does not have external IP addresses. However, Applicant submits that using DHCP to cause hosts to refer to a particular DNS is not the same as "converting ...DNS names into corresponding IP addresses according to data in the enhanced access control list" as stated in Applicant's claim 1.

At least one difference can be illustrated by comparing how Droms and Applicant will process an attempt by a user who is not authorized to access an undesirable host (as is known in the art, a "host" may be a Web page, and may also include hosts which are not web-related, e.g., database servers). Droms will cause a particular DNS (i.e. a DNS having only local DNS names and addresses) to convert the DNS name of the requested undesirable host into a corresponding IP address, and if the DNS has no corresponding IP address, an error message is returned. (See Col. 12, lines 55 – 65.) In sharp contrast, Applicant has disclosed using an Enhanced Access Control List including DNS names that a particular user is prevented from accessing. In Applicant's method as recited in the pending claims, the undesirable host's DNS name in the Enhanced Access Control List is converted by the DNS to a corresponding IP address. The corresponding IP address is added to the access control list (claim 1) or the dynamic access control list (claim 9). The access control list or dynamic access control list, is used (for example by a router) to prevent communication between the user and the undesirable host. This comparison has shown that, unlike Droms, Applicant "converts ... DNS names into corresponding IP addresses according to data in the enhanced access control list."

The Examiner's response to Applicant's argument that Droms does not teach or suggest a method of developing an access control list is accepted because Droms does update an access control list. However, Applicant maintains that Droms' updating of an access control list as referenced by the Examiner (Col. 13, lines 1-24) does not anticipate or render obvious Applicant's method for developing an access control list as stated in claim 1. Droms discloses a different method. In particular, Droms does not reference an enhanced access control list when developing Droms' access control list.

Further, Applicant respectfully disagrees with the Examiner's response to Applicant's argument that Droms does not teach or suggest converting user names into corresponding IP and physical addresses according to data in the enhanced access control list. Applicant acknowledges that Droms checks the "user and user group associated with the IP address" information that is stored in map 114 in the DHCP server (Droms Col. 13, lines 10-13). However, Applicant submits that checking user/IP address relationships in the data structure stored in the DHCP server is not the same as "converting ... user names into corresponding IP and physical addresses according to data in the enhanced access control list" as stated in claim 1. At least one difference is that Droms' map 114 is not an "enhanced access control list" as disclosed by Applicant. Droms' map 114 is not an access control list at all, and thus it cannot be an enhanced access control list. In order to be an access control list, Droms' map 114 would have to contain a list of devices authorized or denied access to a network – but that is not the case. Droms mentions an access control list 146 on the gateway host 142, and another in the AAA server 132. But Droms does not state or imply that map 114 is an access control list, furthermore, map 114 is not an enhanced access control list. Therefore, Droms does not anticipate or render obvious "converting ... user names into corresponding IP and physical addresses according to data in the enhanced access control list" as stated in Applicant's claim 1.

The Examiner states that, regarding claims 9 and 10, Droms fails to disclose mapping user names to IP addresses. However, the Examiner states that Donaldson discloses a method for converting user names into corresponding IP addresses. The Examiner then concludes that it would have been obvious for one of the ordinary skill in the art at the time the invention was made to include the method of converting user names into corresponding IP address as taught by Donaldson in the system of Droms et al. to covert user names and physical addresses into IP addresses. The Examiner states that one is motivated as such in order to determine an IP address with minimum latency to route an information packet based on user name and physical address.

Regarding the Examiner's remarks relating to Applicant's argument that Donaldson does **not** teach or suggest converting user names into corresponding IP and physical addresses according to data in the enhanced access control list – Applicant respectfully submits that the Examiner's remarks do not address Applicant's argument. Applicant's argument was in regard to converting user names, but the Examiner's response pertained to "mapping physical LAN interface (physical address) to logical interfaces (IP address)" and vice versa (Col. 13, lines 18-49). Assuming that the Examiner inadvertently omitted a clarifying part of the remark, Applicant notes that (within the reference supplied by the Examiner) there is a reference to translating a "name" to an IP address at Col. 13, lines 28 -29. However, Applicant respectfully points out that the "name" refers to the "name of the proxy server from the MX record." (Col. 13, lines 27 – 28.) This "name" is not a "user name" as disclosed by Applicant. One of ordinary skill in the art would know that the name of a proxy server in an MX record is a "host name," which is not a "user name" as disclosed by Applicant.

The Examiner added a remark that Donaldson discloses "a method for dynamically updating and storing the IP addresses in access list for performing access verification during the address lookup process (col 9, lines 4-18, co[l] 19, lines 37-54)." Applicant respectfully submits that the reference is clearly distinguishable from Applicant's invention as recited in claim 9 and does not supply the deficiency in Droms. Applicant acknowledges that Donaldson updates a list of IP addresses used as an access list, but the updates are based on Active Filtering tests (Col. 9, line 18) not "generating a dynamic access control list from the enhanced access control list..." as recited in Applicant's claim 9.

Further, it is submitted that if one skilled in the art were to combine Droms with Donaldson in the manner suggested by the Examiner, such combination would render an updated access control list based on Active Filtering that is missing at least (not including the numerous deficiencies in Droms pointed out by Applicant in previous responses): 1) generating a dynamic access control list from the enhanced access control list; and 2) converting user names into corresponding IP and physical addresses according to data in the enhanced access control list.

Thus, it is submitted that Applicant's invention as defined in independent claims 1 and 9, as well as in the claims depending ultimately therefrom, is not anticipated, taught or rendered obvious by Droms or Donaldson, either alone or in combination, and patentably defines over the art of record.

Applicant notes with appreciation the Examiner's indication that claims 18 – 25 are allowed.

In summary, claims 1-25 remain in the application. It is submitted that Applicant's invention as set forth in these claims is in a condition suitable for allowance.

Further and favorable consideration is requested. If the Examiner believes it would expedite prosecution of the above-identified application, the Examiner is cordially invited to contact Applicant's Attorney at the below-listed telephone number.

Respectfully submitted,

DIERKER & ASSOCIATES, P.C.

/Julia Church Dierker/

Julia Church Dierker
Attorney for Applicant
Registration No. 33368
(248) 649-9900, ext. 25
juliad@troypatent.com

3331 West Big Beaver Rd., Suite 109
Troy, Michigan 48084-2813
Dated: January 9, 2009
JCD/JBD